

AD-A247 330



NAVAL POSTGRADUATE SCHOOL

Monterey, California



DTIC
ELECTE
MAR 12 1992
S B D

THESIS

TRANSMISSION CONTROL PROTOCOL/
INTERNET PROTOCOL FOR THE PC:
AN ETHERNET IMPLEMENTATION

by

Pamela H. Patrick

September, 1991

Thesis Advisor:

Norman F. Schneidewind

Approved for public release; distribution is unlimited

92 3 10 148

92-06407



Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE			
1a. REPORT SECURITY CLASSIFICATION		1b. RESTRICTIVE MARKINGS	
2a. SECURITY CLASSIFICATION AUTHORITY		3. DISTRIBUTION/AVAILABILITY OF REPORT	
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE		Approved for public release; distribution is unlimited.	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)		5. MONITORING ORGANIZATION REPORT NUMBER(S)	
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b. OFFICE SYMBOL (If applicable) 55	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School	
6c. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000		7b. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c. ADDRESS (City, State, and ZIP Code)		10. SOURCE OF FUNDING NUMBERS	
		Program Element No	Project No
		Task No	Work Unit Accession Number
11. TITLE (Include Security Classification) TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL FOR THE PC: AN ETHERNET IMPLEMENTATION			
12. PERSONAL AUTHOR(S) Patrick, Pamela H.			
13a. TYPE OF REPORT Master's Thesis	13b. TIME COVERED From To	14. DATE OF REPORT (year, month, day) 1991, September, 26	15. PAGE COUNT 64
16. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
17. COSATI CODES		18. SUBJECT TERMS (continue on reverse if necessary and identify by block number)	
FIELD	GROUP	SUBGROUP	
		TCP/IP, Ethernet, Local Area Network, 3Com, Internetworking	
19. ABSTRACT (continue on reverse if necessary and identify by block number) This thesis will provide an overview of the hardware and protocols required for the implementation of the communications package Transmission Control Protocol/Internet Protocol for the PC. A User's Manual is included as an appendix. The manual is specifically written for use in the Administrative Sciences Department Informations Systems laboratory at the Naval Postgraduate School.			
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS REPORT <input type="checkbox"/> DTIC USERS		21. ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL Norman F. Schneidewind		22b. TELEPHONE (Include Area code) (408) 646-2719	22c. OFFICE SYMBOL AS/Ss

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted
All other editions are obsoleteSECURITY CLASSIFICATION OF THIS PAGE
Unclassified

Approved for public release; distribution is unlimited.

Transmission Control Protocol/
Internet Protocol for the PC:
An Ethernet Implementation

by

Pamela H. Patrick
Lieutenant, United States Navy
B.A., Tulane University, 1984

Submitted in partial fulfillment
of the requirements for the degree of

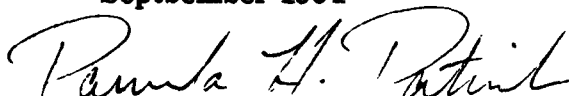
MASTER OF SCIENCE IN INFORMATION SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL

September 1991

Author:

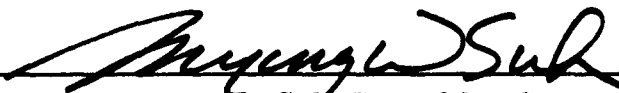


Pamela H. Patrick

Approved by:



Norman F. Schneidewind, Thesis Advisor



Myung W. Suh, Second Reader



David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

This thesis will provide an overview of the hardware and protocols required for the implementation of the communications package Transmission Control Protocol/Internet Protocol for the PC. A User's Manual is included as an Appendix. The manual is specifically written for use in the Administrative Sciences Department Information Systems Laboratory at the Naval Postgraduate School.

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

TABLE OF CONTENTS

I. INTRODUCTION	1
A. PURPOSE OF THE THESIS	1
B. ORGANIZATION OF THE THESIS	1
II. BACKGROUND	3
A. LOCAL AREA NETWORKS	3
B. INTERNETWORKING	3
1. The Goal of Internetworking	4
2. Advantages of Internetworking	6
3. Problems of Internetworking	6
III. HARDWARE	8
A. ETHERNET	8
1. Ethernet Hardware	9
a. Ethernet Cable	9
b. Tapping into the Ethernet	11
c. Repeaters	13
d. Routers	13
2. Ethernet Implementation at the Naval Postgraduate School	14

B.	3COM	15
1.	3Server3	16
2.	3Com Connectivity	18
C.	CONNECTING 3COM TO THE ETHERNET BACKBONE ..	19
IV.	THE TCP/IP PROTOCOL SUITE	21
A.	ISO 7-LAYER REFERENCE MODEL	22
1.	Layer 1: Physical Layer	24
2.	Layer 2: Data Link Layer	24
3.	Layer 3: Network Layer	25
4.	Layer 4: Transport Layer	25
5.	Layer 5: Session Layer	26
6.	Layer 6: Presentation Layer	26
7.	Layer 7: Application Layer	27
B.	TCP/IP	27
1.	Internet Protocol	28
a.	The IP Datagram	29
b.	Routing	31
c.	Internet Control Message Protocol	32
2.	Transmission Control Protocol	33
a.	Reliable Stream Transfer	34
b.	Windows	34
c.	Ports and Sockets	35

V. APPLICATION PROTOCOLS	37
A. TELNET	37
1. Network Virtual Terminal	37
2. Telnet Services	38
3. Telnet Options	39
B. FILE TRANSFER PROTOCOL	39
1. FTP Parameters	40
2. FTP Services	41
C. SIMPLE MAIL TRANSFER PROTOCOL	42
1. SMTP Elements	43
2. SMTP Service	43
VI. CONCLUSIONS AND RECOMMENDATIONS	45
A. MAIL SERVICES	45
B. PERFORMANCE MONITORING	45
C. WIDER IMPLEMENTATION	45
APPENDIX	47
LIST OF REFERENCES	56
INITIAL DISTRIBUTION LIST	57

I. INTRODUCTION

A. PURPOSE OF THE THESIS

University computer laboratories and similar academic and research facilities have traditionally experimented with new combinations and applications of hardware and software. The Administrative Sciences Department Information Systems laboratory at the Naval Postgraduate School (NPS) is no exception. Current research being conducted at NPS in alternative communication connectivity between local area networks and the Internet is the subject of this thesis. This thesis examines the hardware, protocols, and applications associated with the implementation of the software package TCP/IP for Personal Computers. Additionally, a comprehensive User's Manual for this software will be presented.

B. ORGANIZATION OF THE THESIS

This thesis has been divided into six chapters with one appendix. The first chapter discusses the purpose of the thesis and presents an overview of its organization. Chapter II provides a brief background by discussing the topic of internetworking, its advantages, problems, and other related issues. The hardware associated with the implementation is presented in Chapter III, including information on Ethernet hardware, local area network hardware, and

the connection of the two. Chapter IV discusses the two major protocols involved in this system--Internet Protocol (IP) and Transmission Control Protocol (TCP)--and examines the functionality of the two protocols, as well as their place in the International Organization for Standardization's Reference Model for Open System Interconnection. Chapter V provides an explanation of the three application protocols used by the Transmission Control Protocol/Internet Protocol for the PC software: File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Telnet. Chapter VI summarizes the main points made by the thesis and offers recommendations for future research. Finally, the appendix contains the user's manual developed for Transmission Control Protocol/Internet Protocol for the PC.

II. BACKGROUND

A. LOCAL AREA NETWORKS

A local area network (LAN) is a communication network normally used by a single organization over a limited distance. LANs operate over distances up to a few thousand meters at high speeds, usually ranging between four megabits per second and one hundred megabits per second. Many vendors produce the hardware and software required to implement a LAN, each potentially different in its method of connectivity, way of communicating, and strategy for network management. Each, however, strives for the same goal--the sharing of resources. LANs have been desired and created at organizations primarily for one reason--to save money and provide greater flexibility in the use of such resources as laser printers, scanners, hard drives, software, and shared databases. Recently, many LAN managers have realized the shortcomings in limiting resource sharing to their own internal LAN, and are considering the opportunities available on other networks. The question has been, how is it possible to connect this multitude of different networks?

B. INTERNETWORKING

The answer to the question stated above lies in *internetworking*, a technology that "makes it possible to interconnect many disparate physical

networks and make them function as a coordinated unit." (Comer, 1991) Internetworking allows LANs to interconnect regardless of individual physical makeup by hiding the details of network hardware, thus permitting networks to communicate. Figure 1 provides a theoretical diagram of internetworking, showing a number of interconnected LANs participating in a network of networks--an internet.

1. The Goal of Internetworking

The goal of internetworking is "to define an abstract, hardware independent networking environment that makes it possible to build distributed computations that interconnect ... without knowing the details of underlying technologies." (Comer, 1991) Hiding the technological differences between networks makes the interconnection independent of the underlying hardware. For this goal to be reached, two technical requirements must be met:

1. End systems (computers, terminals) must share a common set of communication protocols so they can interoperate.
2. The suite of protocols used for this purpose must support an internetworking capability in a mixed network environment. (Stallings, 1988)

A protocol can be defined as "a formal description of message formats and the rules two or more machines must follow to exchange those messages." (Comer, 1991) A detailed description of the protocols involved is

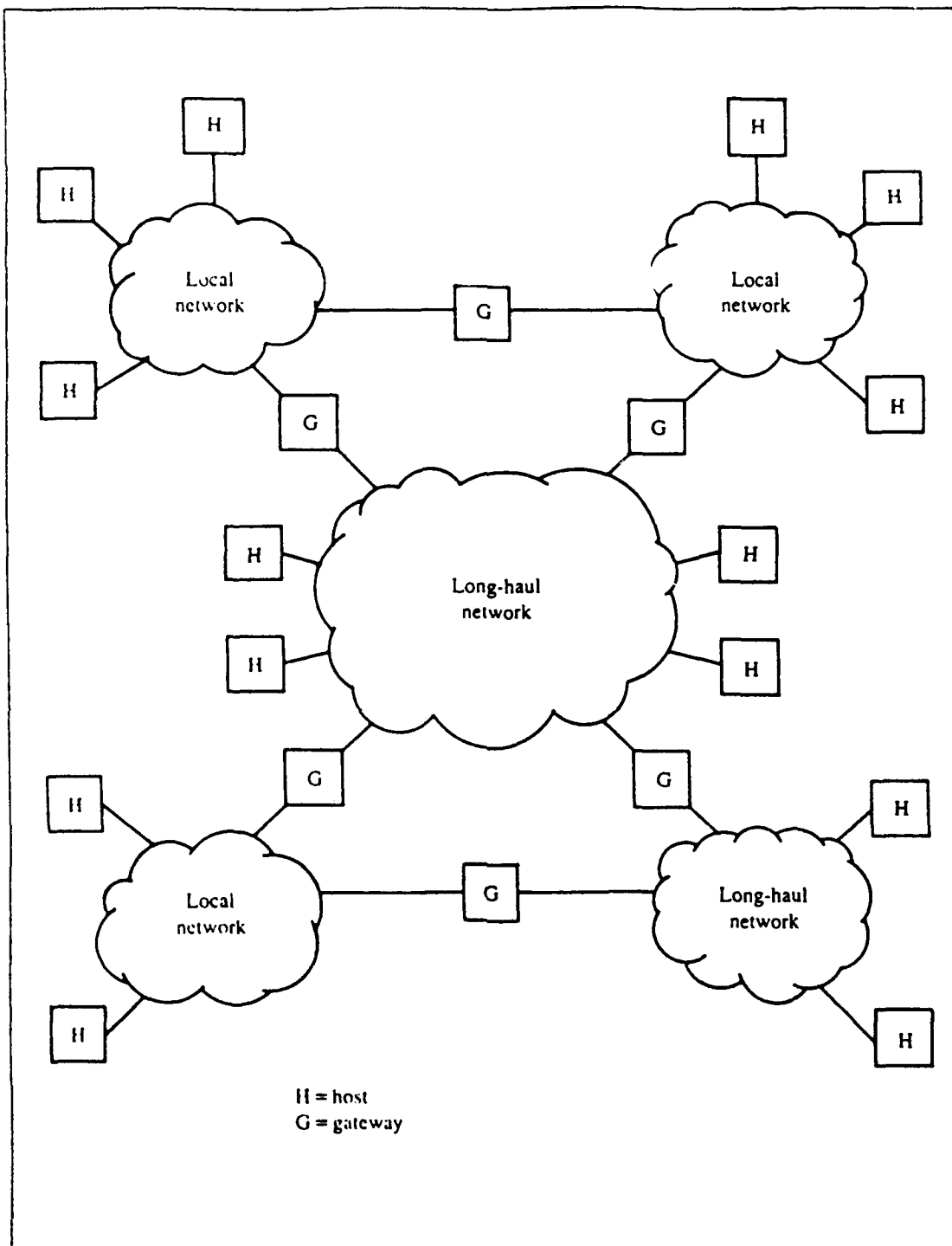


Figure 1: An Internet (Stallings, 1988)

provided in Chapter IV. For now, it is enough to understand that the protocols operate to allow disparate networks to communicate.

2. Advantages of Internetworking

Resource sharing was previously discussed as one of the driving forces behind the proliferation of internetworking. It is clear that sharing data, peripheral devices, and other such resources can provide a great advantage in the effective operation of an organization. Another advantage of internetworking is message communication, the ability to send messages by computer. Message communication is greatly valued by busy executives, academicians, and other professionals, tired of endless games of phone tag. A third advantage of internetworking is its ability to provide interconnection independent of a network's underlying technology, thus allowing an organization to select network hardware to best suit individual needs.

3. Problems of Internetworking

Internetworking allows communication across great divides, both in the geographical sense and in terms of different network technologies, through the use of protocols. If there was just one set of protocols used, internetworking would be a relatively simple process. Unfortunately, there are nearly as many protocols and variations on protocols as there are vendors of network hardware. One of the requirements discussed in section one, above, was for computers to share a common set of protocols. Obviously, if two

networks are attempting to communicate with two different protocols, interconnection will not be possible. One solution to this problem is to choose a standard protocol. Such a standard would ensure interoperability, and would have accompanying benefits of eased procurement, vendor productivity and competition (Stallings, 1988). The Internet Protocol (IP) and Transmission Control Protocol (TCP), commonly referred to as the TCP/IP suite, are the most frequently used protocols today. The TCP/IP suite is thought by many to be an appropriate choice for a standard, and is one of the topics discussed in this thesis (Stephenson, 1990).

III. HARDWARE

A. ETHERNET

Ethernet is a local area network developed by Xerox in the early 1970s. An Ethernet frame carries identification information called a header that allows computers on the network to send the frame to the correct destination. Subdividing messages into frames results in lower costs and greater efficiency because multiple communications between machines sharing the network can proceed concurrently, thus requiring fewer interconnections. A disadvantage, of course, is that as network activity increases, the network capacity must be shared among a larger number of communicating computers. (Comer, 1991)

The Ethernet is a 10 Mbps bus technology with best-effort delivery and distributed access control (Comer, 1991). Bus technology means that the computers connected to a network share a single communication channel. Devices are connected by cables that run between them, but do not pass through a centralized controller mechanism. Because there is no central controller, messages travel directly to and from the intended computer on a bus.

The Ethernet access mechanism--Carrier Sense Multiple Access with Collision Detect (CSMA/CD)--is a distributed access control scheme because no central authority grants access. The CSMA portion of the mechanism operates

to decide whether or not a message can be sent. When a user wishes to send a message, CSMA listens to see if it can detect a carrier-sense signal from another user. If no other signal is detected, the message is sent. The obvious problem with this scheme is that two network users could listen, detect no signal, then begin transmission at the same time, resulting in a collision. When a collision occurs, the CD part of the mechanism detects the collision, and informs both computers to repeat the transmission. To prevent both users from trying to retransmit at the same time, Ethernet uses exponential backoff which randomly calculates the time to wait until retransmission in order to prevent another collision.

1. Ethernet Hardware

Ethernet hardware can be implemented in any number of configurations. The basic components of an example configuration--Ethernet cable, taps, repeaters and routers--are discussed below.

a. Ethernet Cable

Ethernet uses a baseband coaxial cable as its transmission medium. Baseband mediums are typified by signals sent across the cable's serially--one bit at a time--without modulation. Baseband coaxial cable has a single channel and can transmit only a single message at a time. The cable, shown in Figure 2, has a carrier wire at its center and is surrounded by insulation and shielding. Approximately 1/2 inch in diameter, the cable can

be up to 1500 feet (500 meters) long (Comer, 1991). "Called the ether, the cable itself is completely passive; all the active electronic components that make the network function are associated with computers that are attached to the network." (Comer, 1991)

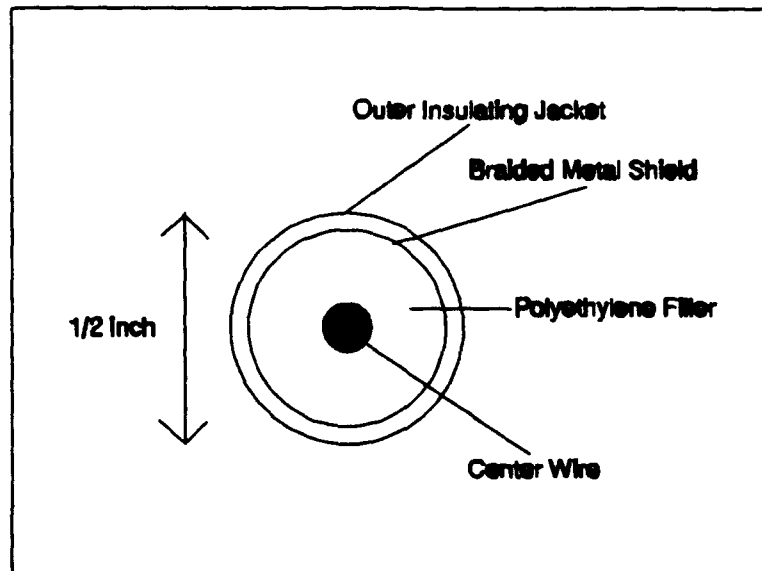


Figure 2: Ethernet Coaxial Cable

A variation of the standard Ethernet cable is thin-wire Ethernet, which is only 1/5 an inch in diameter and cannot be greater than 1000 feet (300 meters) in length (Schatt, 1990). The thinner cable is less expensive than the standard Ethernet cable, but is more flexible and easier to handle. Thin wire Ethernet has three main disadvantages: it is limited to shorter distances, supports fewer connections than standard Ethernet cable, and renders the network inoperative when a computer is either removed from or inserted in the

network. However, the thin-wire does allow direct connection to single boards in computers, making it easier to connect machines to the network. (Comer, 1991)

The ether's single channel is suitable for data transmission, but does not allow integrated voice, data and video. For many implementations, however, this disadvantage is outweighed by Ethernet's advantages. As an accepted IEEE standard (802.3), Ethernet's baseband cabling is a popular choice for LANs (Comer, 1991), because, due to its physical construction, it is easy to tap into the cable. This advantage allows new devices to be added to the network with a minimum of disruption. In the past, connections required that the cable be cut; currently, connections can be made with pressure taps that allow small pins to touch the center wire and the braided shield (Shoch, 1982).

b. Tapping into the Ethernet

Connecting or tapping into the Ethernet requires two components: a transceiver and a host interface. Shown in Figure 3, the transceiver connects directly to the center wire and braided shield of the Ethernet cable. The transceiver has two main functions. First, the transceiver's analog hardware that allows it to sense and send signals on the ether. Second, the transceiver's digital hardware allows communication with a digital computer. (Comer, 1991)

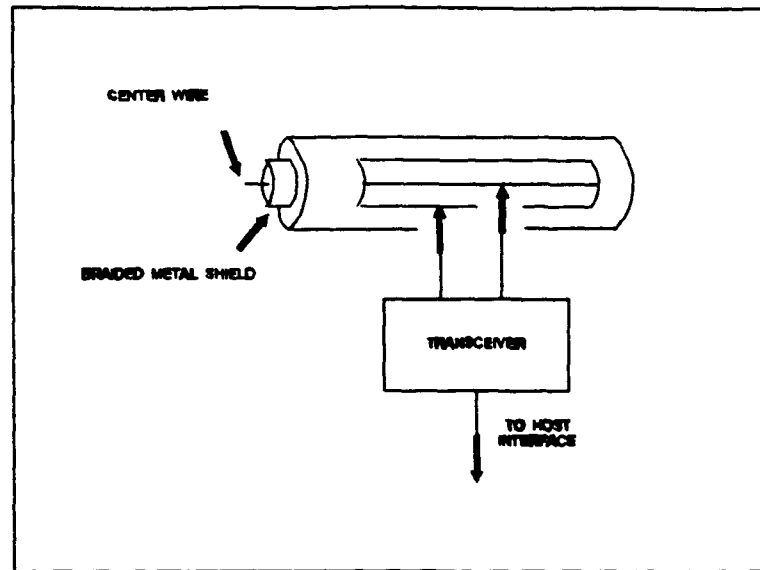


Figure 3: Electrical Connection at a Tap

The second component necessary for tapping into the ethernet-- the host interface--connects to the transceiver and communicates with the computer. "Each host interface controls the operation of one transceiver according to instructions it receives from the computer software." (Comer, 1991) Four major functions include:

1. transferring transmit data from the controller to the transmission system
2. transferring send data from the transmission system to the controller
3. indicating to the controller that a collision is taking place
4. providing power to the transmission system (Shoch, 1982)

Together, the transceiver and the host interface allow a successful connection between a computer and the ether, and provide the means for the computer to control its use of the ether.

c. Repeaters

A repeater is a device that rebroadcasts a signal to prevent signal degradation. Repeaters are used to extend the length of the transmission system past the limits of the transmission medium alone. A maximum of two repeaters can be placed between any two machines, thus still limiting the total length of the network.

Use of a repeater to extend the total length of an Ethernet has both advantages and disadvantages. In addition to the inherent advantage of increased network length, repeaters are the least expensive method of extension. The repeater restores the signal and extends the transmission distance by restoring and reshaping the received signal. A disadvantage lies in the fact that repeaters are active electronic components requiring power to operate, and therefore can fail in inconvenient places and at inconvenient times. (Comer, 1991)

d. Routers

A router is a device that interconnects two networks and passes messages between them. Routers use a standard protocol to determine the destination of a message and over which path to send it. Because routers can

choose the path that is quickest, or has the lightest load, they are said to perform dynamic path allocation. (Comer, 1991) "They tend to be most prevalent and work best in nationwide academic and government installation, where hundreds of links run TCP/IP." (Fitzgerald (1), 1984)

2. Ethernet Implementation at the Naval Postgraduate School

The implementation of Ethernet at the Naval Postgraduate School pertinent to this thesis is as the campus backbone. At the Naval Postgraduate School, the backbone is a thick Ethernet cable that spans the campus. Many of the academic departments' individual LANs are connected to this backbone, including the 3Com network implemented in the Administrative Sciences Department's Information Systems laboratory. Also connected are the Computer Center's and Computer Science Department's computers.

The backbone is connected to the Internet through a router located in the Computer Center in Ingersoll Hall. The router is in turn connected to a Packet Switching Node (PSN), a computer dedicated solely to switching packets. The PSN attached to the router in the Computer Center switches packets destined for or transmitted by networks or other computers attached to the Naval Postgraduate School backbone. This configuration is depicted in Figure 4.

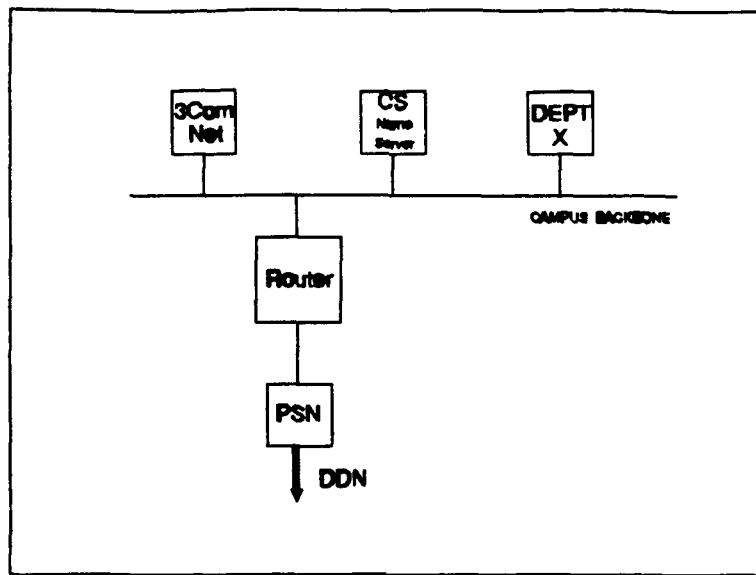


Figure 4: Naval Postgraduate School's Ethernet Backbone

B. 3COM

The 3Com network is an Ethernet-based local area network located in the Administrative Sciences Department Information Systems laboratory in Ingersoll Hall, room IN-224. The 3Com LAN shares the Ethernet characteristics of Carrier Sense Multiple Access/Collision Detection and exponential backoff discussed in Chapter III, Section A. The implementation of 3Com in IN-224, shown in Figure 5, connects five IBM PC XTs, a 3Server3 server, a printer, and a plotter via a thin-wire Ethernet bus. The details of this connection are discussed below.

The software used to run the 3Com network includes Ethershare, Etherprint, Ethermail, and Ethermenu. Ethershare allows the computers

connected to the network to share the server's resources; it is the software interface of the 3Com network. Its main purpose is to permit sharing of the server's hard disk. User computers may create their own volumes, or subdivisions of the hard disk, for their own use. The Ethershare software permits designation of the volumes as public, private or shared, depending on the security level desired by the user. Etherprint allows the user computers access to a single shared printer, controlling the process so that files are printed in the order they arrive and do not get scrambled if they arrive at the same time. Ethermail allows messages to be sent and received by user computers. The network server acts as a mailbox, delivering or holding the mail depending on whether or not the intended recipient is powered on. Ethermenu operates a network menu system, allowing users to select among such options as Utilities, DOS and Print menus. (Andersland, 1989; Schatt, 1990)

1. 3Server3

The 3Server3 is a special purpose server that can not be used as a user computer. The server's functions include sharing peripheral devices, networking and internetworking capabilities and coordination of multiuser network software (3Server3, undated). The 3Server3 has no keyboard, floppy disk drive or monitor; all operational settings are accomplished using a thumb wheel and switch, and the only display is a small LED read out. This unique configuration has both advantages and disadvantages. Greater security is one

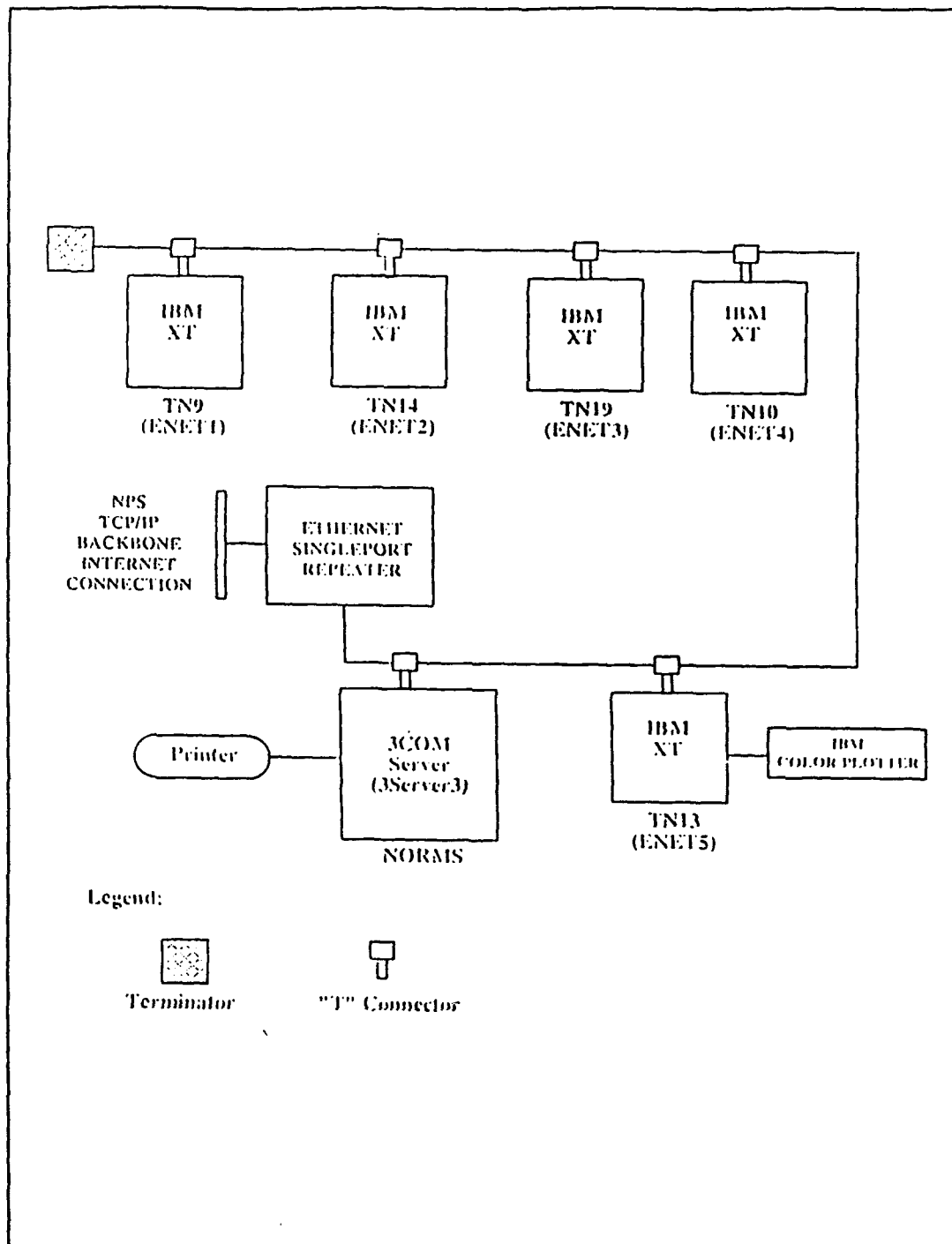


Figure 5: 3Com Network Implementation in IN-224

benefit as users do not have access to the server and cannot attempt to use it as a workstation. The major detriment to the setup is that if the server fails, another personal computer cannot be substituted for it, greatly decreasing the system flexibility. (3Server3, undated; Schneidewind (1), 1991)

2. 3Com Connectivity

The 3Com network connection requires Etherlink cards, BNC cable connectors, T-adapters and terminators. The 3Com Etherlink card is installed in each user computer, and functions to send and receive information across the network. The T-adapters are the basic connection between the thin-wire Ethernet cable and the computers. The base of the T-adapter connects to the Etherlink card in the back of each user computer. Using a BNC cable connector, the thin-wire Ethernet cable is plugged into the two arms of the T-adapter. These connections are displayed in Figure 6. The T-adapter allows greater flexibility in connecting and disconnecting computers to the network because if a T-adapter is removed from an Etherlink card connection, electrical continuity still exists and the network continues to function. However, if a cable is disconnected, the circuit is broken and the network stops working. Similarly, if a terminator, required at each end of the network bus, is removed, the circuit is again broken and the network ceases to function. (Andersland, 1989; Schneidewind (1), 1991; Schatt, 1990)

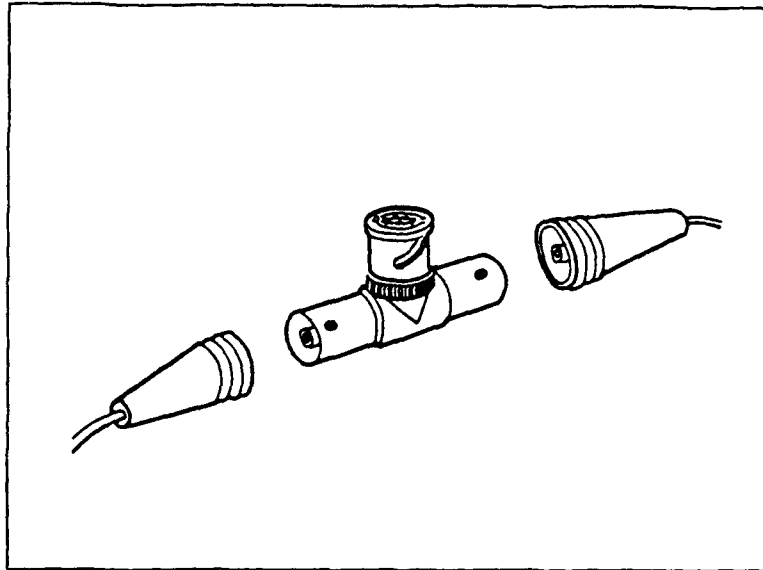


Figure 6: Connecting Cable to a T-adapter

C. CONNECTING 3COM TO THE ETHERNET BACKBONE

To permit communication outside its own network, 3Com was connected to the campus Ethernet backbone and through the router to the internet. The problem of connecting a thin-wire Ethernet LAN, such as 3Com, to a thick-wire Ethernet backbone can be solved by providing an interface between the two. This interface has been implemented using a transceiver connected to the thick-wire campus Ethernet backbone. An Access Unit Interface cable connects the transceiver to a thick-thin repeater, replacing one terminator. (Schneidewind (2), 1991)

The hardware requirements and physical connectivity of an Ethernet based local area network have been established. The next step in

understanding the internetworking process is to examine the protocols under which the process operates.

IV. THE TCP/IP PROTOCOL SUITE

Protocol was defined in Chapter II as a set of rules to be used by machines when communicating: required to initiate, maintain and terminate communications. All protocols contain the following components:

1. The *syntax* of a protocol defines the bit stream by dividing it into a series of fields much like that used by application programmers in laying out a record.
2. The *semantics* of a protocol define the meaning of each field in the bit stream.
3. *Timing* of the protocol pertains to both the data rate of the bit stream and any pauses between acknowledgements during half duplex communications. (Fitzgerald (2), 1990)

Conceptually, protocol software can be thought of as modules arranged in layers, each having responsibility for a part of the communication task. "Layered protocols are designed so that layer *n* at the destination receives exactly the same object sent by layer *n* at the source." (Comer, 1991) There are many benefits to the layered approach to protocol design:

1. Network software and hardware engineers can allocate tasks among network resources more easily and effectively because the functions are delineated clearly.
2. Network managers can assign responsibilities in their departments more effectively. With the layered structure, responsibilities are delineated more clearly than they otherwise might be.

3. Because the modular design is based on the seven layers, it is easier and less costly to replace a network layer with its equivalent product from another vendor. This, of course, presupposes that the other vendors follow the same seven-layer approach.
4. Upgrading a network is easier and less time consuming because individual layers can be replaced. Normally an upgrade replaces an entire set of software.
5. Networks can be converted to both international and industry standards on a progressive layer-by-layer basis. As the standards for one layer become available, they can be implemented while leaving the remaining layers intact. This phase-in approach is both easier to debug and more palatable to network operations personnel who do not have to learn an entirely new system at one time.
6. Many network functions can be offloaded from the host mainframe to the front end processor or some other network control device. This promotes a distributed architecture that increases overall processing speed. (Fitzgerald (2), 1990)

This chapter examines the two primary protocols for internet communication discussed in the previous chapter--Internet Protocol and Transmission Control Protocol. It begins with a discussion of the International Organization for Standardization (ISO) Seven-Layer Reference Model, hereafter referred to as the ISO model. (Comer, 1991)

A. ISO 7-LAYER REFERENCE MODEL

An introduction to the ISO model is presented in Figure 7. The basic communication tasks performed by each layer are described, as well as analogies to Post Office letter handling and conversation, intended to make the process more clear. The seven layers are present at both ends of the

ISO Seven-Layer Model for Data Communications	Post Office Letter Handling Compared to Using the ISO Model	One Person Speaking to Another Compared to Using the ISO Model
Application layer (layer 7): Provides network services such as file transfer, terminal emulation, and logging into a file server.	Establishes contents of the letter, including text and graphics.	Establishes subject to be discussed, expression to be used, and knowledge to be assumed.
Presentation layer (layer 6): Performs encryption, code conversions, format conversions so incompatible devices can talk, and so forth.	Performs translation of the letter to another language and ensures secrecy if necessary.	Handles language differences, such as English to Spanish, and ensures secrecy if necessary.
Session layer (layer 5): Manages the session, synchronizes data flow establishes and terminates the session, and so forth.	Writes name, address, and zip code of both the sender and receiver of the letter.	Commands attention and recognizes other person, establishes and terminates conversation at the intellectual level.
Transport layer (layer 4): Provides end-to-end control, adds sequence numbers, acknowledgements, and some error recovery.	Handles certified or registered mail, verifies receipt of the letter.	Identifies the other person. Controls speed of ideas as you think, as opposed to voice speed.
Network layer (layer 3): Establishes links to other networks, maintains and terminates switched connections, handles packets, and routes messages between different networks.	Handles sending the letter outside the U.S. postal system to another country. Puts the letter contents onto a piece of paper (packet).	Identified the location of the other person. Assembles ideas (packet) before structuring them into sentences.
Data link layer (layer 2): Establishes a link in the network and transfers data in a frame, detects and corrects errors, handles flow control between modems, and sequences messages.	Handles sending the letter to someone within the U.S. postal system. Puts the piece of paper (packet) into an envelope (frame) and corrects misdeliveries.	Establishes the physical path the voice is to take (through the air or over a telephone circuit). Assembles sentences (frames) and corrects misunderstandings.
Physical layer (layer 1): TRANSMIT. Physically moves data bits between modems and circuit activation or deactivation. ALL physical movement of data bits takes place at this level.	MAIL. Moves the letter by airplane, truck, ship, and the postal delivery person.	SPEAK. Send your ideas by speaking. Voice speed (how fast you speak) versus the external noise and the movement of your voice through the air.

Figure 7: ISO Seven-Layer Model (Fitzgerald (1), 1990)

communication link. "The actual message data bits must move down from layer 7 to layer 1, across the communication circuits that interconnect layer 1 at the host end to layer 1 at the terminal end, and then back up to layer 7 at the other end of the communication link." (Fitzgerald (1), 1990) Physical communications occur only at layer 1--the physical layer. Connections between the remaining layers are known as *virtual* links; they are only theoretical--no data bits move between them. The following sections provide more in-depth explanations of each of the seven layers. (Fitzgerald (1), 1990)

1. Layer 1: Physical Layer

The physical layer governs the movement of data bits over a communication circuit. Such items as electrical voltage, timing, half duplex/full duplex circuits, and rules for initial connection and disconnection are controlled at this layer. The most important function of the physical layer is to determine how the host and receiver will define a 1 bit and a 0 bit so that both ends recognize them. (Fitzgerald (1), 1990; Fitzgerald (2), 1990)

2. Layer 2: Data Link Layer

The physical layer provides the data link layer with recognizable data bits which the data link layer assembles into data frames. The data link layer adds flags to indicate the beginning and ending of messages, and ensures these flags are not misinterpreted as data. Layer 2 also identifies and corrects damaged, lost and duplicated data frames and ensures subsequent layers

receive error-free frames. "Major functions include error detection and correction, retransmission instructions for erroneous messages, definition of message boundaries, resolution of competing requests for the same data link, and flow control." (Fitzgerald (2), 1990) (Fitzgerald (1), 1990; Fitzgerald (2), 1990)

3. Layer 3: Network Layer

The network layer of the ISO model is concerned with packet switching. It takes messages from the fourth layer and repackages them as packets, before sending them to the lower two layers where they are transmitted. The network layer also performs addressing and routing. Packets are addressed and directed to their destination, while routing is accomplished using dynamic tables that contain frequently updated circuit routes. The tables are updated to indicate overloaded or down circuits. The network layer attempts to optimize network utilization and circuit flow by picking the best route using the information from the tables. (Fitzgerald (1), 1990; Fitzgerald (2), 1990)

4. Layer 4: Transport Layer

The transport layer ensures that the packets formed in the network layer are delivered in sequence, error-free, without losses or duplications. "The transport layer is often called the host-to-host layer or end-to-end layer because it establishes, maintains and terminates 'logical' connections for the

transfer of data between end users." (Fitzgerald (1), 1990) The layer deals with end-to-end issues such as network addressing, multiplexing several messages into one circuit, and regulating the flow of information by controlling the movement of messages. Once communication extends beyond the transport layer, communication issues become visible to the end user. (Fitzgerald (1), 1990; Stallings, 1988)

5. Layer 5: Session Layer

The session layer is concerned with network management, with primary responsibilities including initiating, maintaining, and terminating a session. Users on the network are recognized through the session layer. In particular, users communicate directly with this layer, which can verify a password, transfer files between equipment, and enable a switch from a half-duplex to full-duplex circuit. The session layer can also handle recovery from a system crash, monitor system usage, and bill users for their time. (Fitzgerald (1), 1990)

6. Layer 6: Presentation Layer

The presentation layer of the ISO model is concerned with the formatting function, file transfers and network security. Format choices include data code and character set (eg., ASCII or EBCDIC), video screen formatting, encryption and compaction. "Its job is to accommodate the totally different interfaces seen by a terminal in one node and what is expected by the

application program at the host mainframe computer." (Fitzgerald (1), 1990)
(Fitzgerald (1), 1990; Stallings, 1988)

7. Layer 7: Application Layer

The application layer provides the end user access to the network. Network programs found at the application layer include electronic mail, database managers, application diagnostics and processor sharing. "The application layer provides a means for application processes to access the ISO environment." (Stallings, 1988) (Fitzgerald (1), 1990; Stallings, 1988)

B. TCP/IP

The ISO model provides a framework for consideration of communication protocols. "The four lower layers are guides for moving and receiving information between two systems; the three upper layers are concerned with setting up and performing applications." (Fitzgerald (1), 1990) This section examines how the TCP/IP protocol suite uses the ISO model to perform communication tasks.

Layered network protocols, like the ISO model described above, are designed to reduce the complexity of application programs by dealing with common issues in the protocol layers. Complex systems do not use just one protocol to handle all communication tasks; instead, they use a set of cooperative protocols sometimes referred to as a protocol family or protocol suite. The TCP/IP protocol suite includes a variety of protocols that perform

distinct services necessary for communication between and control of otherwise incompatible computers and networks. These protocols include Internet Control Message Protocol, File Transfer Protocol, Telnet, and Simple Mail Transfer Protocol. These protocols will be discussed in detail in both this and the next chapter. (Carr, 1990; Comer, 1991)

1. Internet Protocol

The Internet Protocol is responsible for accepting data from one machine or network and sending it across the internet until the data reaches its destination. The IP scheme is an unreliable, best-effort, connectionless message delivery system, called the IP datagram. It is unreliable because delivery is not guaranteed. The protocol makes an attempt--a best-effort--to deliver packets. The internet does not discard packets on a whim; the unreliable nature of the protocol comes into play when resources are exhausted or underlying networks fail. It is said to be connectionless because each packet is treated independently from all others. A sequence of IP datagrams making up a message may be sent over different paths; some may be lost while others are delivered. The IP connectionless approach provides a number of advantages, including flexibility, robustness, and connectionless application support. Because IP can use a number of different paths, one malfunctioning path will not prevent a message from being delivered. (Comer, 1991; Stallings, 1988)

The basic definition required to implement a layered network protocol is provided by IP, which defines the basic unit of data transfer used by a TCP/IP internet. Also, IP performs the routing function, choosing the paths the data will follow to their destination. Finally, IP includes a set of rules that embody the idea and implementation of unreliable packet delivery. (Comer, 1991)

a. The IP Datagram

The basic unit of transfer in IP is the datagram. The protocol takes the data it is presented to transmit and adds a special header containing control and addressing information. The format of an IP data frame can be seen in Figure 8, while the special data that make up the header are summarized below.

- Version: version number
- IHL: length of header
- Type of service: specifies reliability, precedence, delay, and throughput parameters
- Total length: total datagram length, including header
- Identification: unique identifier for datagram's source, destination, and user protocol
- Flags: indicates fragmentation
- Fragment offset: indicates where in the datagram this fragment belongs
- Time to live: measured in 1-second increments
- Protocol: next level protocol to receive datagram

- Header Checksum: error detection device
- Source address: sender network and station
- Destination address: receiver network and station
- Options: encodes user requested options
- Padding: ensures header ends on a 32-bit boundary
- Data: data field, must be a multiple of eight bits in length, total length of data field plus header is a maximum of 65,535 octets

Because IP is a datagram based service, each packet can be handled and routed independently. The routing of the IP datagrams is described below.
(Stallings, 1988; Stephenson, 1990)

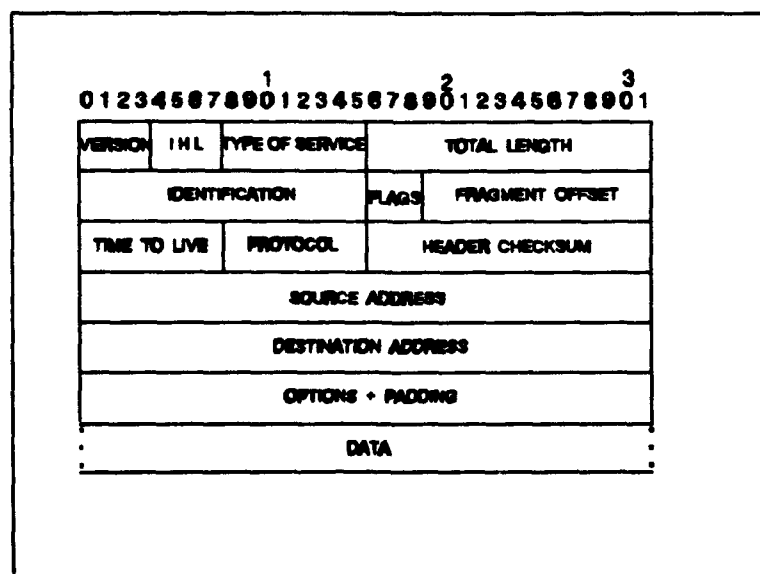


Figure 8: IP Datagram

b. Routing

The connectionless feature of the IP service allows datagrams to take different routes through the Internet. There are two types of routing: direct and indirect. In direct routing, the datagram is transmitted directly from one machine to another. This is the basis for the packet delivery system of the Internet. Indirect routing occurs when a datagram's destination is not on a directly attached network; the sender must pass the datagram onto the Internet for delivery. The choice of how to send a datagram across the multiple networks that make up the Internet is made by the IP routing algorithm. (Comer, 1991; Fitzgerald, 1990)

The IP routing algorithm uses an Internet routing table that contains information on possible destinations and how to reach them. It is easy to imagine that if every machine stored the address of every other, the resulting table would be immense and impossible to use efficiently. To keep the routing tables of a manageable size and able to make routing choices efficiently, the information stored contains network addresses, not individual host addresses. Once a datagram reaches the correct network, the network's own protocols intervene to ensure the datagram reaches its intended host. (Comer, 1991)

In addition to the processing of outgoing datagrams, IP handles the routing of datagrams intended for its host. An incoming IP datagram is examined by IP to determine if it is indeed intended for local delivery. If it is

addressed to the host's IP address, the IP software on the host accepts the datagram and passes it to TCP for further processing. If the IP's host is not the intended recipient, the host must destroy the datagram. Errors such as this are passed on the system by Internet Control Message Protocol. (Comer, 1991)

c. Internet Control Message Protocol

Internet Control Message Protocol (ICMP) is a utility protocol that allows systems to report errors or information regarding unexpected circumstances to one another, check one another's status, and perform simple routing updates. Since ICMP is a required part of IP, it must be included in every IP implementation. The error reports are passed only to the source of the datagram; the source must report errors to the involved application problem and take steps to correct the problem. The problems in the communication environment on which ICMP reports include: "... when a datagram can't reach its destination, when the gateway doesn't have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route." (Stallings, 1988) (Comer, 1991; Stallings, 1988)

An ICMP message is passed across the Internet in the data portion of an IP datagram. The header of the datagram is used to indicate its ICMP status. Types of ICMP messages include: destination unreachable, time exceeded, parameter problem, source quench, redirect, echo, echo reply,

timestamp, and timestamp reply. The ICMP echo request or 'ping' can be used to test whether a specific destination is reachable and responding. Because both the echo and echo reply ICMP messages are passed in an IP datagram, receipt of an echo reply indicates that the system is working correctly. (Comer, 1991; Stallings, 1988)

The unreliable nature of IP means that there is no guarantee that the destination will receive packets, the data will be intact, or the packets will be in the correct order. To find these guarantees, we must look at another layer of the TCP/IP suite, the Transmission Control Protocol.

2. Transmission Control Protocol

Transport protocols, such as TCP, provide a reliable method for the exchange of data between processes, ensuring data is delivered error-free, in the order that it was sent, and without loss or duplication. Its basic role is providing reliable end-to-end data transfer between two processes, called transport users (including File Transfer Protocol, Telnet, and Simple Mail Transfer Protocol). The role of TCP also includes defining some system parameters to ensure dependable data transfer. These parameters include the format of the data and acknowledgement exchanged to produce a reliable transfer, procedures to be used to ensure data arrives correctly, how communicating machines handle such errors as lost or duplicated packets, and how TCP stream transfer is properly initiated and terminated. (Comer, 1991)

a. Reliable Stream Transfer

The reliable stream delivery service provided by TCP guarantees that a stream of data sent across the internet will arrive error-free and without duplication or loss of data. This service is based on two practices: positive acknowledgement with retransmission and sequence numbering. Positive acknowledgement with retransmission ensures that a packet is retransmitted if the timer expires before acknowledgment is received. To prevent duplication and misordering of packets, TCP assigns each packet a sequence number. The sequence number is included in the acknowledgement sent, so the sender knows which packets have been received. If a packet arrives out of order, it can be reordered by sequence number; if lost, the destination TCP will not acknowledge its receipt, and the sending TCP will resend the packet. (Carr, 1990; Comer, 1991)

b. Windows

The simple positive acknowledgement scheme described above wastes a great deal of network potential because the sender must wait to receive an acknowledgement before sending the next packet. The TCP has solved this problem by using a sliding window protocol. Under this scheme, shown in Figure 9, the sender may send multiple packets before waiting for an acknowledgement. The size of the window constrains the number of packets that can be unacknowledged at a given time. "Because a well tuned sliding window protocol keeps the network completely saturated with packets, it

obtains substantially higher throughput than a simple positive acknowledgement protocol." (Comer, 1991) The sliding window mechanism used by TCP provides both efficient transmission and end-to-end flow control. By using a variable size window, the receiver has the ability to limit transmission according to the amount of buffer space available to accommodate more data. (Comer, 1991)

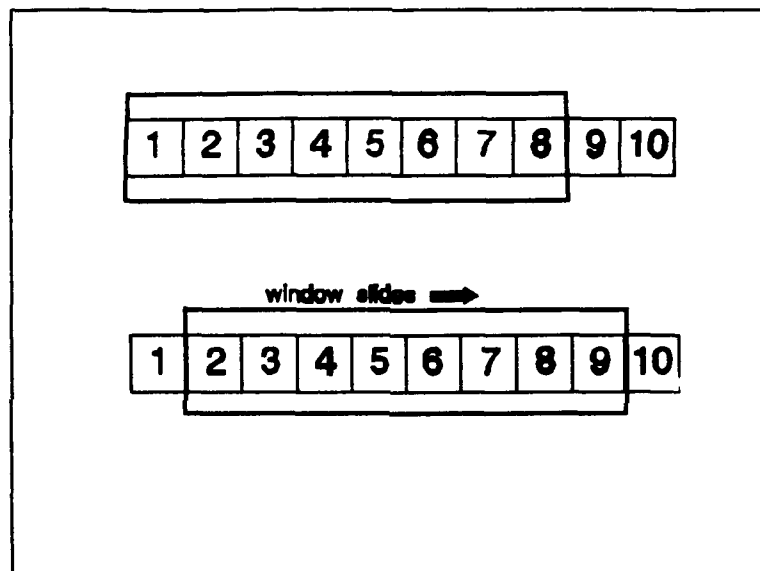


Figure 9: Sliding Windows

c. Ports and Sockets

The addressing scheme used by TCP has three levels. At the first level, TCP begins the address with an application or program, which TCP calls a process, and a unique address. The process address is combined with the address of its originator and forms a new, complex address called a port. The

port is then added to an internet address to form a socket. Each socket is unique throughout the internet, consisting of a specific process running on a specific node in a specific network. Transport service by TCP is provided by means of a logical connection between a pair of sockets, or endpoints. Because TCP views its communications as a connection between a pair of endpoints, a given TCP port can be shared by multiple connections, increasing system capacity. (Comer, 1991; Stallings, 1988)

V. APPLICATION PROTOCOLS

The IP and TCP protocols described in Chapter IV provide the basic transport services of the internet. This chapter will continue the discussion of the TCP/IP suite by examining three of its application protocols: Telnet, File Transfer Protocol, and Simple Mail Transport Protocol.

A. TELNET

The objective of Telnet is to "provide a general, bi-directional character-oriented communications facility between terminal devices and terminal oriented processes." (Stallings, 1988) Telnet allows terminals to connect to and control applications running in a remote host as if it were a local user of the host. The service provided by Telnet is termed transparent because it gives the user the impression of direct connection to the remote machine. The basic idea behind the Telnet remote login service is the network virtual terminal. (Comer, 1991; Stallings, 1988)

1. Network Virtual Terminal

The Telnet protocol provides terminal access to remote hosts via network virtual terminal (NVT). A NVT is a virtual device, not a physical one, which standardizes a few simple terminal functions. Logging on to a remote host could pose a problem if the characteristics of the terminal requesting access are not known or supported by the remote host. The NVT concept

solves this problem with mechanisms that allow the involved machines to agree upon the language they will use for data transfer, and by performing translations between the agreed upon language and the terminal's native mode. This allows the host freedom from having to maintain information about other terminal types. (Comer, 1991; Stallings, 1988)

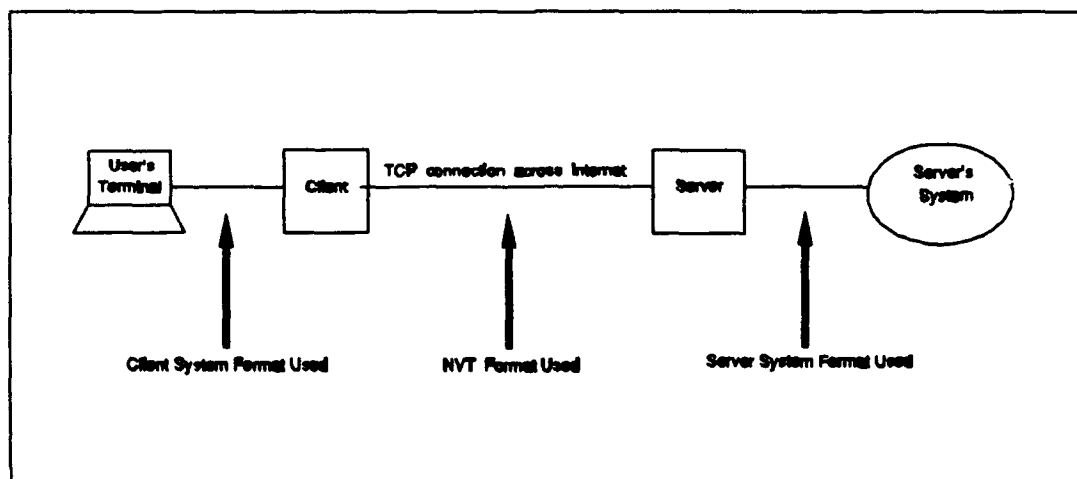


Figure 10: A Network Virtual Terminal Implementation

2. Telnet Services

Telnet uses the NVT concept to allow a user at a terminal connected to the local host to use programs at a remote host as if the user were a local user of the remote host. There are two parts to this process: the user module and the server module. The user module in the local host interacts with its terminal input/output processor to provide translation of terminal characters to the language agreed upon via NVT for data transfer. The server module in the remote host interacts with the requested processes or applications, and serves as a terminal handler to make remote terminals look as if they are

local. Telnet treats both ends the same; instead of forcing one side to make the connection, it allows either side to become a user, and either side can negotiate options. (Carr, 1990; Comer, 1991; Stallings, 1988)

3. Telnet Options

One of the most powerful and flexible capabilities Telnet presents to users is the ability to negotiate transfer options. Telnet has defined standard options that can change the virtual terminal characteristics, or the transfer protocol. Some of the most common negotiated options are: transmit binary, echo, status, timing-mark, terminal-type, and end-of-record. Because Telnet option are negotiable, it makes it easier for either end of the communication to reconfigure the connection. Since all Telnet software understands the basic NVT protocol, users and servers can communicate even if they do not recognize the exact same set of options. (Comer, 1991; Stallings, 1988)

B. FILE TRANSFER PROTOCOL

The File Transfer Protocol (FTP) is the most frequently used of the TCP/IP application protocols, and accounts for much network traffic (Comer, 1991). The FTP relies on the error-free reliable stream service provided by TCP to send files to or get files from another computer. The set of agreements and procedures that make up FTP specify how the information, or files, should be transferred between computers on the internet. (Stallings, 1988)

1. FTP Parameters

The parameters defined by FTP for data storage and transfer include data type, transmission mode, and data structure. Data can be of two types: text and non-text. Text data can be in either the ASCII or EBCDIC character sets. Non-text data types can be either image or logical byte size. Image data structure is used for data exchange between similar computers. It is most often used with files that are executable programs, function libraries, and other files that have been translated or compiled, and will be used only by another computer with the same processor type. Logical byte size data structure is used for the same types of files as image data, but is used when the file must be interpreted and manipulated on a different type of computer. (Stallings, 1988)

The several file type options allowed by FTP permit easier interface to a variety of file systems on destination computers. File structure is an unstructured string of bytes ending with an end-of-file marker. Record structure involves transmission of individual records, separated by an end-of-record marker. This structure is used when files can be handled more efficiently as records. The final file type, page structure, consists of independent indexed pages that can be separated in transmission and a file descriptor that can locate individual pages. This file type is used primarily in the TOPS-20 system. (Stallings, 1988)

The final parameter used by FTP is transmission mode. These modes refer to the way data will be treated for transmission, and allows for optimal use of the communication network. Stream mode is the simplest of the three modes, and is the default for all transfers. It consists of a stream of bytes with the end indicated by an end-of-record or end-of-file byte. Block mode is more complex than stream mode, and consists of a series of blocks. The benefit of block mode is that if a transmission error is detected, the sender can stop transmission, then restart with the block in which the error was detected. This is accomplished by sequencing the blocks, and recording the progress of the transfer by block sequence number. The final transmission mode is compressed mode, in which the file is transmitted with replicated and filler data reduced. The compressed data status is encoded in the message sent, then expanded when it reaches its destination. This mode can sometimes dramatically reduce the number of bits transferred, making the communication more efficient. (Stallings, 1988)

2. FTP Services

The primary service provided by FTP is, as its name suggests, file transfer. This is accomplished by interaction between a user FTP process and a server FTP process. The user FTP process initiates the connection, provides authentication to the remote host, specifies file(s) to be transferred, and transfers data in cooperation with the server FTP process. The server FTP

process responds to the initial connection, sets up parameters for transfer and storage, and manages the transfer. (Comer, 1991; Stallings, 1988)

As well as file transfer, FTP provides a number of other services, including interactive access, format specification and authentication control. The interactive access service allows humans to interact easily with remote servers, and oversees the mechanics of the file transfer process. The format specification service allows the user the choice of type and format of data to be stored. System security is enhanced by the authentication control service, which requires users to gain access using a login name and password. (Comer, 1991)

C. SIMPLE MAIL TRANSFER PROTOCOL

Electronic mail (e-mail) is one of the most popular office automation components. It allows elimination of telephone tag session, and reduces the multitude of office paperwork. The basic e-mail system must perform four function: creating, sending, receiving and storing. In an internetworking sense, e-mail is treated as part of the layered protocol approach, using lower layer protocols to transmit messages. The e-mail protocol in the TCP/IP suite is Simple Mail Transfer Protocol (SMTP). The focus of SMTP is on how the underlying mail delivery system passes messages across the internet. However, SMTP does not specify the interaction between the local mail system

and the user, how mail is stored, and how often the local mail system attempts to send messages. (Comer, 1991; Stallings, 1988)

1. SMTP Elements

The standard for SMTP messages has two parts: the header and the body. With two exceptions, SMTP doesn't care about the format or content of these messages. The two exceptions are the requirement to use standard seven-bit ASCII, and the addition of log information to the beginning of the message telling the path it took. There are a number of elements basic to the SMTP process. One element is the standard mailbox specification, or address, in the form of `user@domain`, where the user identifies a specific account or mailbox in the domain, and domain identifies a specific host. A similar format is used when path information is added to the beginning of an SMTP message. Another element of the SMTP service is its command structure. These commands manage the activities on the underlying TCP connection, and include such commands as `helo`, `mail`, `rcpt`, `send`, and `quit`. Coded replies are also an element of SMTP service, indicating whether the response is good, bad, or incomplete, and the type of error that occurred. (Stallings, 1988)

2. SMTP Service

The SMTP activity in a single mail transfer can be broken into three phases. In the first phase--connection setup--the connection is readied for use. The sequence for connection setup is first, the sender opens a TCP connection

to the receiver, then both ends identify themselves. The next phase is mail transfer, consisting of one or more transactions, each concerning a single piece of mail. The mail transfer has three functions: the originator of the message is identified, the intended recipient is identified, and the actual data transfer takes place. The final phase closes the connection by the sending machine issuing a quit command, waiting for a reply, then initiating a TCP close operation for the connection.

VI. CONCLUSIONS AND RECOMMENDATIONS

This thesis has provided an overview of the hardware and protocols pertinent to the implementation of the Transmission Control Protocol/Internet Protocol for the PC software package. Though the basic implementation is complete, there are still a number of issues that require further research.

A. MAIL SERVICES

One of the decisions that must be made when implementing a mail service in a LAN is how to handle addressing issues. Choices include each node having its own address, all mail directed to the network server, or addition of a dedicated mail server. Research should be conducted to evaluate these alternatives, and to recommend the best choice for the 3Com implementation.

B. PERFORMANCE MONITORING

Monitoring the performance of the software will provide valuable information to the network managers. Statistics gathered could be used to identify needed corrections and modifications, allowing system optimization.

C. WIDER IMPLEMENTATION

Implementation of the Transmission Control Protocol/Internet Protocol for the PC software package on another network, perhaps the IBM token-ring

network in Ingersoll Hall room IN-224, should be considered. This would allow comparison of the software's operation and efficiency on an ethernet LAN versus a token-ring LAN.

APPENDIX

Transmission Control Protocol/Internet Protocol for the PC USER MANUAL

This appendix is a user manual for the Transmission Control Protocol/Internet Protocol for the PC software package. The manual is specifically written for use in the Administrative Sciences Department Information Systems laboratory located in Ingersoll Hall room IN-224.

TCP/IP FOR THE PC

A Basic Reference Guide

For use on the

Administrative Sciences/Information Systems

(AS/IS) Computer Laboratories

3Com Local Area Network in I-224

I

ntroduction to Local Area Networks

A local area network (LAN) is a group of microcomputers or other workstation devices located in the same general area and connected by a common cable. A LAN is designed to interconnect microcomputers, terminals, minicomputers, and other hardware, for the purpose of communicating among themselves and alternately with a host mainframe computer or public network.

The most common reason for developing a LAN is resource sharing. Networks allow the sharing of peripheral devices such as hard drives, printers, and scanners. Application programs such as spreadsheets, word processing, and communication packages, can be shared so that multiple copies are not necessary. Databases can also be shared in such a way that multiple microcomputers can have access to a single database. This capacity for sharing hardware and software resources allows greater flexibility and cost savings in the use of expensive computer peripherals and software.

The basic components of a LAN are the server computer, the user computer(s), and the interconnecting cabling system. The server is usually a microcomputer that is specifically designated to act as the network server. The server performs only those functions required of a network server; it is not accessed by users wishing to work on the network. Server functions include repository of software programs, network management, printer and other peripheral device management, and database repository.

The user computer is normally a microcomputer or terminal, and is connected to the server by a cabling system. A simplified schematic of a typical connection is shown in Figure 1. One server can support more

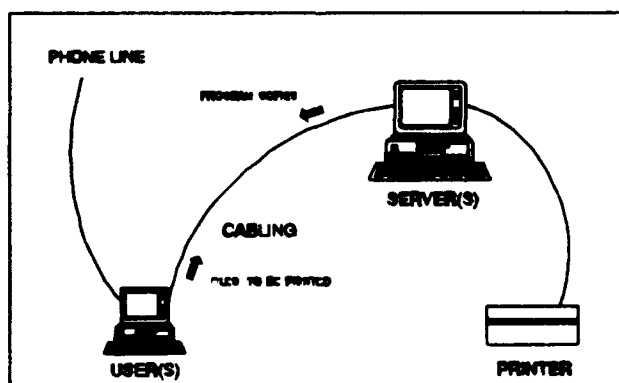


Figure 1: LAN Schematic

than one user computer; usually six to ten. The cabling system connecting the server and the users can be present in a number of forms and configurations. Cabling can be twisted pair wire, coaxial cable, or fiber optic cable. Configurations include bus, ring and star.

Logging on to a LAN as a user gives access to all the shared software on the server. When a software package is chosen, a copy of the software is downloaded to the user computer for execution. The user computer executes the software like a stand-alone computer, not accessing the server again unless a peripheral device, such as a printer, is needed. Further information on these and other local area network topics can be found in the references listed below.

Suggested References

Fitzgerald, J., Business Data Communications, John Wiley & Sons, Inc., 1990.

Schatt, S., Understanding Local Area Networks, Howard W. Sams & Company, 1990.

TCP/IP FOR THE PC

This user's manual will provide a "quick and dirty" introduction to the use of the software package Transmission Control Protocol/Internet Protocol (TCP/IP) for the PC. It will cover the major functions of the software, including file transfer and remote login. A more detailed guide to the operations of the software, and functions for more advanced users can be found in the full user guide in the documentation rack in IN-224.

The following conventions will be used in presenting the commands and subcommands for TCP/IP for the PC. Command lines will be shown in the following format:

name [-options] [parameters]

The command **name** will be shown in bold letters. Some commands have options, which are typed in preceded by a "-". Some commands also have mandatory or optional parameters. If the options or parameters are displayed in [], they are optional; if not, they are required. Commands are not case sensitive, but options are



Getting Started

1. Turn on your computer and log onto the network (following the instructions provided at your terminal). You will see the batch file (files with .BAT extensions, that execute application programs) listings for the various applications available on the network.
2. Highlight the TCPIP.BAT file and press the **Enter** (also called the **Return**) key.



File Transfer

The **FTP** command allows you to transfer files to and from a remote host. FTP allows you to transfer both ASCII and binary files. The command operates from an FTP command shell.

You can specify the host to which you want to connect, and several other options from the command line. The command line is:

ftp [-bdhloq?] [host]

where:

- host** - character string name or internet address in standard format of a foreign host. The **ftp** command immediately attempts to establish a connection to an **ftp** server.
- b** - displays the number of bytes being transferred
- d** - toggles debugging mode, default is off
- h** - toggles hash-sign (#) printing. Default is off. A # is printed for every 1024 bytes transferred.
- l** - starts logging to file **FTP.LOG**
- o** - overwrites local files without verification. This condition occurs if the name specified for the file being received already exists. This option should be used with care.

For example, to open a **ftp** connection to the Naval Postgraduate School (NPS) mainframe with the number of bytes transferred displayed, and logging enabled, you would type:

ftp -bl cc.nps.navy.mil



Subcommands

! [command] [arguments]

puts you back in operating system, allowing you to execute DOS commands. To return to the FTP command shell, still resident in memory, type **EXIT** at the DPS prompt.

ascii

sets the file transfer type to netascii. Netascii is the default transfer type and can be used to transfer files made up of text characters.

binary

sets file transfer type to image and is synonymous with the image subcommand.

bye

synonym for the quit subcommand

cd foreign-directory

provides the same abilities on the foreign host as does the DOS cd command on your PC.

close

terminates FTP connection to the remote server and returns control to the FTP shell

delete foreign-file

deletes the file foreign-file on the foreign host. If you do not specify the foreign-file, the FTP command prompts you to do so.

dir [host-path] [localfile]

displays a listing of the files in the current working directory. If you specify host-path (where host-path is either a path to a different directory or some specific file designation, or both) only those files are displayed. If you specify localfile, the output is written to the file localfile and to the screen. You must specify host-path whenever you specify localfile.

get foreignfile [localfile]

transfers foreignfile to your PC. If you do not specify the localfile, the foreign file name is used (and altered, if possible) to conform to DOS file name restrictions.

help [subcommand]

displays explanatory information and usage of FTP subcommand. If not specified, a list of all subcommands is displayed.

image

sets the file transfer type to image and is synonymous to the binary subcommand. Image type is primarily provided for transfer of binary data (.EXE and .COM files).

lcd [local-path]

changes the current working directory on your PC to that specified by local-path. If you do not give a local-path, the name of the current working directory on your PC is displayed.

open host

establishes a connection to the specified host FTP server where host is either a character string name or an internet address in standard form of a host providing FTP service. If you do not specify host, the FTP command prompts you to do so.

put localfile [foreignfile]

puts the localfile from your PC for storage on the foreign host. If you do not specify foreignfile, the localfile name is used.

quit

terminates the FTP session with the foreign server and exits the FTP command shell.

status

displays the current status for these FTP command parameters: connection (the foreign FTP server), transfer mode, transfer type, form, structure, any flags in effect.

**telnet**

The Telnet command allows you to establish an IBM 3270-interface connection with an IBM host, such as the NPS mainframe, running the VM TCP/IP program. The following command enters the Telnet mode:

telnet name

where name is the character string name or internet address of the foreign host. For example, to establish a Telnet connection to the NPS mainframe, you would type:

telnet cc.nps.navy.mil

Once logged on to a foreign host, the keystrokes **Ctrl]** are used to invoke Telnet functions. The available Telnet functions are:

- ?** displays the help screen
- a** sends "are you there?" inquiry to the target host
- b** sends "break" to the target host
- c** closes the connection and exits from Telnet
- e** sends to target on every typed character
- l** local echo (Telnet echos typed input)
- E** send to target only when end-of-line is typed
- q** exits from Telnet without closing the connection
- r** foreign echo (target host echoes typed input)
- x** sends any outstanding data now
- U** turns on the line-25 clock and status report (default is on)
- u** turns of the line-25 clock and status report

LIST OF REFERENCES

Andersland, D. L., *3Com Etherseries Local Area Network*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1989.

Carr, J., "TCP/IP Protocol Suite," *LAN Magazine*, v. 5, pp. 25-27, November 1990.

Comer, D. E., *Internetworking with TCP/IP Vol 1: Principles, Protocols and Architecture*, Prentice-Hall, Inc., 1991.

Fitzgerald (1), J., *Business Data Communications*, pp. 398-440, John Wiley & Sons, Inc., 1990.

Fitzgerald (2), J., *Business Data Communications Student Study Guide*, pp. 207-212, John Wiley & Sons, Inc., 1990.

Schatt, S., *Understanding Local Area Networks*, pp. 129-153, Howard W. Sams & Company, 1990.

Schneidewind (1), Norman F., Class Handout, IS-3502, January, 1991.

Schneidewind (2), Norman F., Class Notes, IS-3503, March, 1991.

Shoch, J. F., and others, "Evolution of the Ethernet Local Computer Network," *Local Network Technology Tutorial*, pp. 60-76, IEEE Computer Society Press, 1990.

Stallings, W., "Beyond Local Area Networks," *Local Network Technology Tutorial*, pp. 360-364, IEEE Computer Society Press, 1990.

Stallings, W., and others, *Handbook of Computer-Communications Standards Volume 3, Department of Defense Protocol Standards*, pp. 26-188, Macmillan Publishing Co., 1988.

Stephenson, P., "Sweet TCP/IP Suite: Living in a Multiprotocol, Multivendor World," *LAN Magazine*, v. 5, pp. S9-13, November 1990.

3Server3 Guide, pp. 2-1-2-14, 3Com, undated.

INITIAL DISTRIBUTION LIST

- | | | |
|----|--|---|
| 1. | Defense Technical Information Center
Cameron Station
Alexandria, Virginia 22304-6145 | 2 |
| 2. | Library, Code 52
Naval Postgraduate School
Monterey, California 93943-5002 | 2 |
| 3. | Professor Norman F. Schneidewind
Administrative Sciences Department
Naval Postgraduate School
Monterey, California 93943-5002 | 1 |
| 4. | Professor Myung W. Suh
Administrative Sciences Department
Naval Postgraduate School
Monterey, California 93943-5002 | 1 |
| 5. | LT Pamela H. Patrick, USN
Naval Support Force Antarctica Code 10
PSC 467
FPO AP 96531 | 1 |